アプリケーションセキュリティテストと露出管理

# zcrX

## アプリを検査し、修正の優先順位を判断

zcrXは、静的アプリケーションセキュリティテスト（SAST）でソースコードを、動的アプリケーションセキュリティテスト（DAST）で稼働中のアプリを検査します。暗号の移行準備、ソフトウェア脆弱性、依存関係の信頼性も1つのコンソールに集約。登録済みホストとビルドシステム上のAgentがポスチャーを報告し、悪用のシグナル、深刻度、影響ホスト数で修正を優先順位付けします。

提供中・年間サブスクリプション。範囲とお見積もりは承認済みパートナー経由。

**zcrXの評価に適したチーム**・脆弱性管理、アプリケーションセキュリティ、プラットフォームエンジニアリングの各チーム、複数顧客を管理するセキュリティサービス事業者、耐量子暗号への移行を計画するセキュリティ責任者。

### 優先順位付けの用語

**CVE・Common Vulnerabilities and Exposures**
公表済みのサイバーセキュリティ脆弱性を識別するIDとレコードです。[1]

**CISA KEV・Known Exploited Vulnerabilities**
米国のサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）が公開する、実環境での悪用に証拠がある脆弱性のカタログです。[2]

**EPSS・Exploit Prediction Scoring System**
公表済みCVEが今後30日間に実環境で悪用される確率をFIRSTが推定した値です。深刻度ではなく、悪用の可能性を示します。[3]

用語の出典：[1] CVE Program・[2] CISA・[3] FIRST・[1] ↗ [2] ↗ [3] ↗

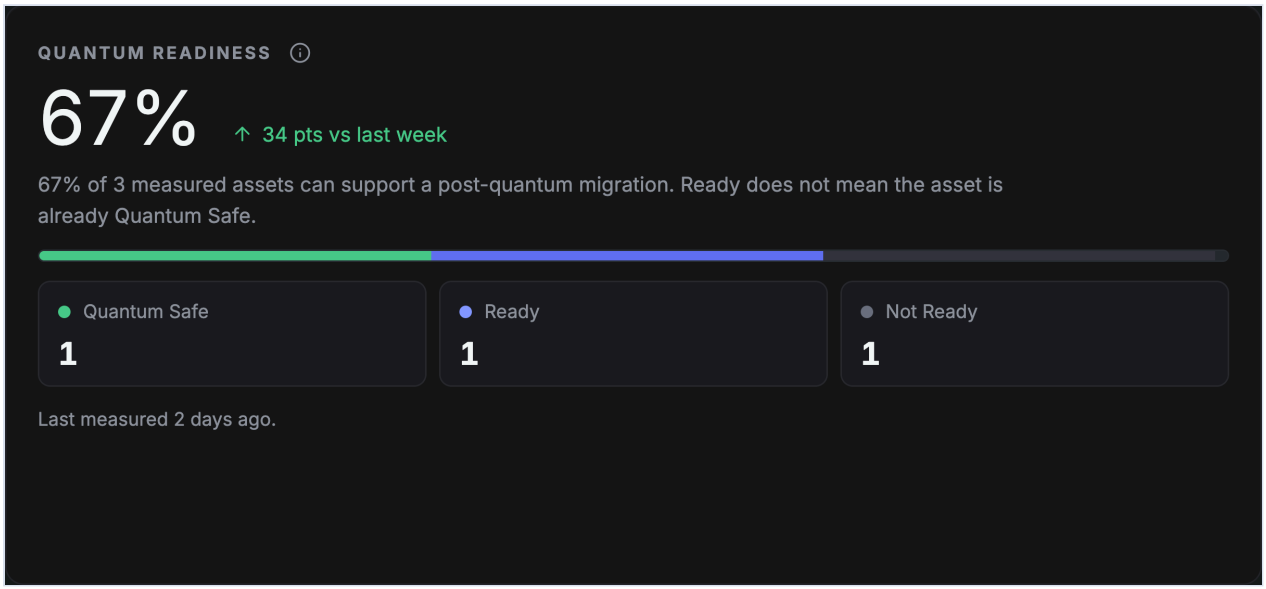
### 各ビューで判断できること

| | |
|---|---|
| **量子時代に備えた暗号** | 証明書とアルゴリズムの一覧をpost-quantum移行の準備状況と照らして追跡します。 |
| **優先順位付きの脆弱性対応** | CISA KEVの状態、EPSSスコア、深刻度で修正の優先順位を決めます。CVEの件数だけでは判断しません。 |
| **検証済みのサプライチェーン** | cryptographic proofまたはAgentによる証明で、複数のエコシステムにわたり依存関係の来歴を確認します。 |
| **プロバイダー向けの一元管理** | 権限委譲とleast-privilegeによるアクセスで、すべての顧客テナントのpostureを管理します。 |

# 移行準備と修正の優先順位を確認

## 01 / 暗号の移行を計画する

Cryptography posture：証明書とアルゴリズムの一覧をquantum-safe・ready・not readyで評価




量子対応の準備状況ウィジェット全体。状態の凡例と、ReadyとQuantum Safeの違いを残しています。 デモ — サンプルデータであり、顧客の実測値ではありません。英語UIを原文のまま掲載。 デモ画面を開く ↗

> 暗号の優先順位は耐量子暗号への移行の緊急度を反映します。この例のReadyは移行準備ができた状態であり、既に耐量子という意味ではありません。事業の文脈が未申告の場合、緊急度はまだ評価できません。

## 02 / 修正が上位になる理由を読む

- Software vulnerability posture：ホストとパッケージのfindingをCVEアドバイザリ、CISA KEVの状態、EPSSスコアに照合
- KEV、スコア、影響を受けるホスト数で修正を優先順位付けし、各順位の理由を提示
- 深刻度別に公開された修正期限に照らしてfindingを追跡し、期限超過を警告

| Why it matters | Action |
| --- | --- |
| A critical advisory affects this package version; An affecting advisory is on CISA's Known Exploited Vulnerabilities catalog | View affected packages |

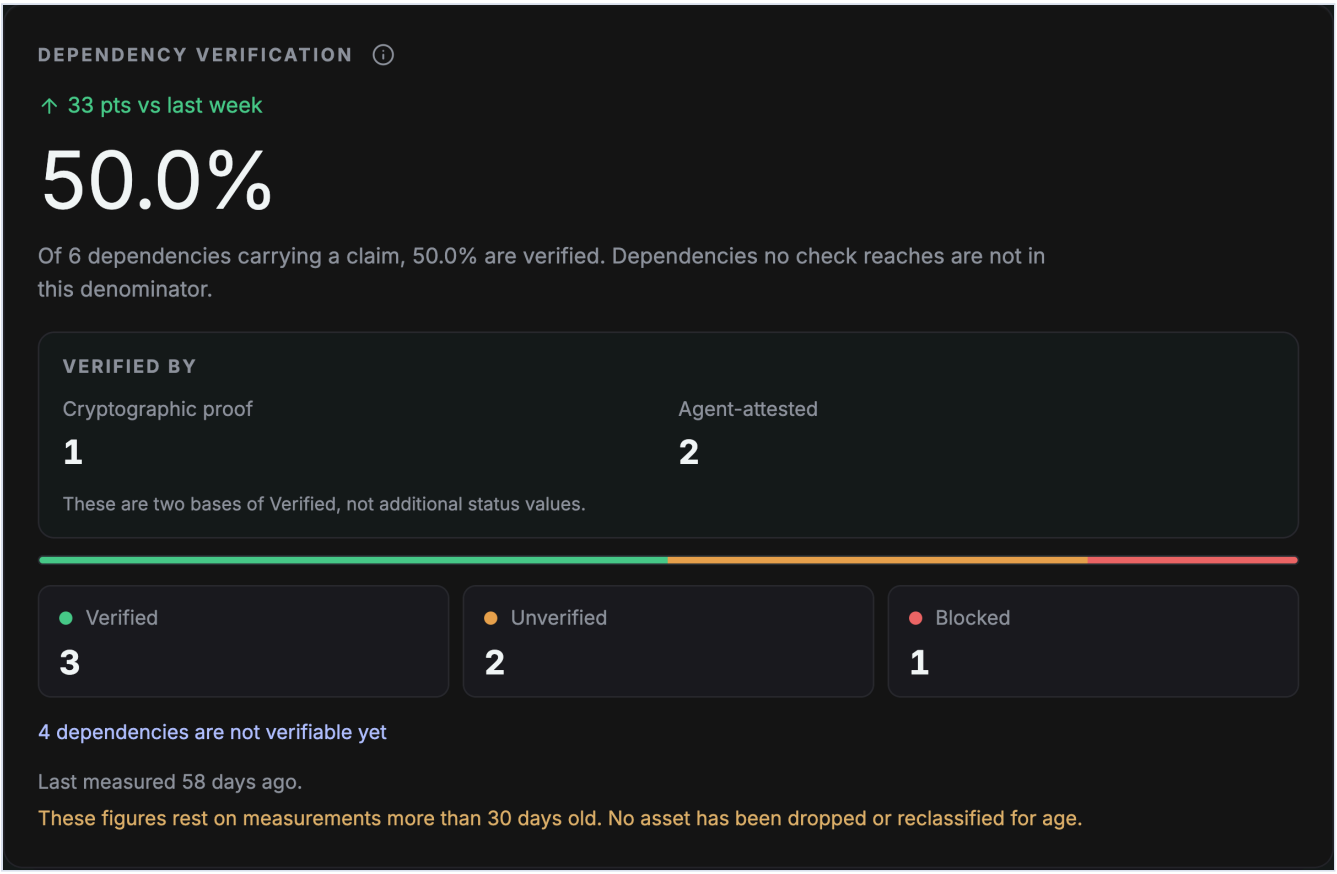
優先行1件の「Why it matters」と「Action」列全体。重大なアドバイザリとKEVへの登録が理由として表示されます。顧客環境で測定した成果ではありません。 デモ — サンプルデータであり、顧客の実測値ではありません。英語UIを原文のまま掲載。 デモ画面を開く ↗

> ソフトウェアビューは、公開済み修正期限と照らした経過日数でもfindingを表示します。元の画面には未評価ホストと修正方法がまだないパッケージもあり、どちらも安全を示す状態ではありません。

# 依存関係の来歴を検証する

## 03 / 証明と証拠不足を区別する

Supply-chain posture：npm、PyPI、Go、Mavenを含むエコシステムでcryptographic proofまたはAgentによる証明で依存関係の来歴を確認




検証ウィジェットの分母、2つの検証根拠、状態の凡例を保持。Agentによる証明と暗号学的証明はVerifiedの根拠で、追加の状態ではありません。最終測定は58日前。30日超の測定値という警告と、古さを理由に除外・再分類した資産はないという注意書きを残しています。 デモ — サンプルデータであり、顧客の実測値ではありません。英語UIを原文のまま掲載。 デモ画面を開く ↗

> この例では、検査が到達しない依存関係は検証率の分母に含めません。Unverified、Blocked、Not verifiable yetは異なる状態です。画面上の割合は、お客様の環境のカバレッジを保証しません。

## パートナーと評価する対象範囲

### npm・PyPI・Go・Maven・Linuxホスト・コンテナイメージ

cryptographic proofまたはAgentによる証明で依存関係の来歴を確認し、エコシステムごとのカバレッジと既知の脆弱性件数を表示します。

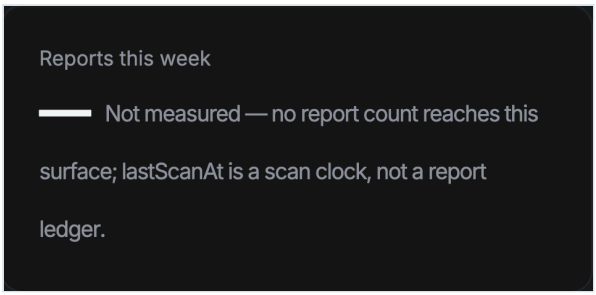
> 承認済み概要には以下のエコシステムと資産種別が記載されています。実際のOSバージョン、イメージ、ビルド環境はパートナーとの検証が必要です。無制限の互換性を保証する一覧ではありません。

# 測定範囲とアクセス権限を把握する

## Agentと測定の境界

ホストとビルドシステムに軽量なAgentを展開し、継続的にスキャン

Agentフリートでは、登録済みAgent、稼働状態、ホストごとの各領域の測定状態を確認できます。Agentのないホストは未測定であり、安全とはみなしません。

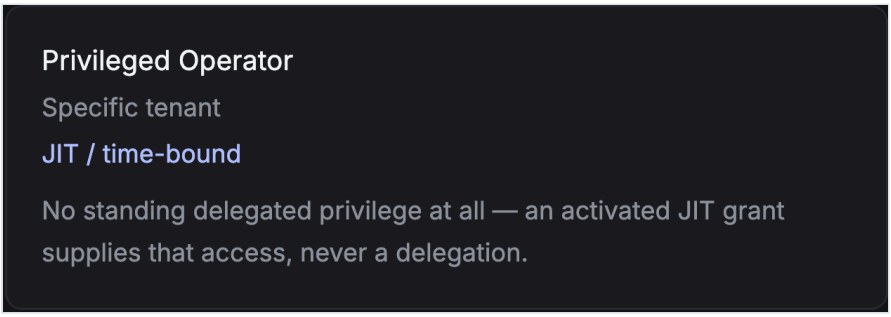



「Reports this week」ウィジェット全体。サンプルはNot measuredと明記し、スキャン時刻とレポート件数を区別しています。 デモ — サンプルデータであり、顧客の実測値ではありません。英語UIを原文のまま掲載。 デモ画面を開く ↗

## アクセスを顧客テナントごとに限定

顧客テナントごとに権限委譲・least-privilege・期限付き（JIT）アクセスを持つマルチテナントのプロバイダー管理画面

プロバイダー管理画面は複数顧客テナントに対応し、権限委譲と最小権限アクセスを提供します。事前承認と、必要時に承認するjust-in-time（JIT）ポリシーがあり、JITアクセスには期限があります。




Privileged Operatorのロールカード全体。このデモでは有効化されたJIT grantがアクセス権を与え、委譲だけでは権限を与えません。元の画面には顧客承認待ちの状態もあります。 デモ — サンプルデータであり、顧客の実測値ではありません。英語UIを原文のまま掲載。 デモ画面を開く ↗

## 運用に必要な詳細も確認

- ソフトウェアごとのプロダクトライフサイクルとサポート終了（EOL）を追跡
- finding、依存関係、Agentフリートのデータを CSVでエクスポート

> CSVはカンマ区切りのデータ形式、EOLは製品のライフサイクル終了を指します。3つのビューは、一時点のスキャンではなくAgentによる継続測定でzcrスイートの対象領域を広げます。

> 一次サポートはチャネルパートナーが担当し、zcrがパートナーを支援します。具体的なサポート条件は確認が必要です。

# 評価範囲を具体化する

## 評価前のよくある質問

**zcrXはもう利用できますか?**

はい。年間サブスクリプションでご利用いただけます。範囲、お見積もり、技術評価はチャネルパートナーが確認します。

**すべてのホストにソフトウェアのインストールが必要ですか?**

zcrXは登録したホストとビルドシステムに軽量なAgentを展開します。Agentのないホストは「未測定」と表示され、安全とはみなされません。

**zcrXはどのように修正の優先順位を決めますか?**

CISAのKnown Exploited Vulnerabilities（KEV）の状態、EPSSスコア、深刻度、影響を受けるホスト数で優先順位を決めます。findingの件数だけでは判断しません。

**複数の顧客環境を管理できますか?**

はい。zcrXには顧客テナントごとに権限委譲とleast-privilegeアクセスを持つプロバイダー管理画面があり、複数の顧客を管理するチャネルパートナー向けに設計されています。

## 承認済みパートナーに共有する情報

| | |
|---|---|
| **資産と導入許可** | 対象アプリ、検査を許可された環境、ホスト、ビルドシステム、バージョンと、検査・Agent導入の承認者を整理します。 |
| **テナント境界** | 顧客テナント、データ所有者、承認者を特定し、委譲する権限と有効期間を合意します。 |
| **確認する証拠** | finding、移行状態、来歴の証拠、CSV出力、未確認・未測定の例を選びます。 |
| **環境の検証** | OSとバージョン、リソース、通信経路、導入権限、容量、必要なアクセスをパートナーに確認します。本書では確定していません。 |
| **商用・提供条件** | エディション、パッケージ、価格、通貨、単位、請求周期、税、適用日、サポート、提供責任をパートナーの提案で確認します。 |

### 技術デモ

公開デモは3領域のポスチャーを表示します。
SAST/DASTの対象アプリと検査環境はチャネルパートナーと合意します。

### 評価範囲のご相談

チェックリストで登録範囲と検証事項を合意し、パートナーから範囲を明示した提案・見積もりを取得します。
契約と提供は承認済みパートナーを通じて行います。

承認済みパートナーに評価を相談する ↗　サンプルデモを見る ↗

デモ — サンプルデータであり、顧客の実測値ではありません。英語UIを原文のまま掲載。